

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/759,443

Filed: January 13, 2001

Docket No.: 10001558-2

Title: PUBLIC KEY VALIDATION SERVICE

REMARKS

The following remarks are made in response to the Office Action mailed March 24, 2005. Claims 1-14, 16-34, and 36-59 were rejected. With this Response, claims 1 and 21 have been amended. Claims 1-14, 16-34, and 36-59 remain pending in the application and are presented for reconsideration and allowance.

Claim Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1-8, 10, 14, 15, 17-28, 30, and 35 as being anticipated by the Ramasubramani et al. U.S. Patent No. 6, 233,577.

The PKVA of amended independent claim 1 includes an off-line registration authority configured to generate a first public key serial number (PKVN) having a high probability of being different from all other PKVNs previously generated by the registration authority. The registration authority is also configured to issue a first unsigned public key validation certificate (unsigned PKVC) off-line to a subject that binds a public key of the subject to the first PKVN. The registration authority is also configured to maintain a certificate database of unsigned PKVCs in which it stores the first unsigned PKVC. A credentials server is configured to issue a disposable public key validation certificate (disposable PKVC) on-line to the subject. The disposable PKVC binds the public key of the subject from the first unsigned PKVC to the first PKVN from the first unsigned PKVC. The credentials server is also configured to maintain a table that contains entries corresponding to valid unsigned PKVCs stored in the certificate database.

Amended independent claim 21 includes similar limitations to those of claim 1 in defining a method for managing the validity status of a subject's public key. The method includes generating off-line a first PKVN having a high probability of being different from all other previously generated PKVNs, issuing off-line to a subject a first unsigned PKVC that binds a public key of the subject to a first PKVN, maintaining a certificate database of unsigned PKVCs in which the first unsigned PKVC is stored, issuing on-line to the subject a disposable PKVC that binds the public key of the subject from the first unsigned PKVC to the first PKVN from the first unsigned PKVC, and maintaining a table that contains entries corresponding to valid unsigned PKVCs stored in the certificate database.

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/759,443

Filed: January 13, 2001

Docket No.: 10001558-2

Title: PUBLIC KEY VALIDATION SERVICE

The Ramasubramani et al. patent does not teach or suggest all of the above limitations of independent claims 1 and 21. The Ramasubramani et al. patent at column 7, lines 33-60 discloses:

It has been described that it takes a noticeable length of time in a regular full-power desktop computer to obtain a certificate from a CA and generate a pair of keys; private and public keys therefor. To minimize the latency of obtaining a certificate with a mobile device, a certificate manager module (CMM) 342 maintains a certificate database, preferably in the database 328, to reserve a list of undesigned but issued certificates, referred to as free certificates, from one or different CAs. Whenever a user account is created to activate a mobile device that requires one or more certificates to access certain web servers requiring a certificate, a certificate request (certRequest) signal is sent to the CMM 342 to fetch needed certificates from the certificate database. Upon receiving the fetched certificates from the certificate database, the CMM 342 assigns the certificates to the particular account by attaching the device ID 316 and other account information, hence the fetched certificates become associated to the particular account and are placed in the certificate list 320. Meanwhile the CMM examines the number of the free certificates available in the certificate database, if the number is below a value, for example 200 certificates, referred to as threshold, the CMM calls the HTTP module 330 to establish a connection to the appropriate CA via the landnet 104 to obtain new free certificates to fill up the certificate database till the level of the threshold is reached, as such there are always sufficient free certificates available in the certificate database to supply any new accounts with the ready-to-use free certificates.

Thus, the Ramasubramani et al. patent disclosed CMM 342 contains a database of a list of undesigned but issued certificates referred to as free certificates to minimize latency of obtaining a certificate with a mobile device. Operating based on a threshold, the CMM obtains new free certificates to fill up the certificate database until the level of the threshold is reached, such that there are always sufficient free certificates available in the certificate database to supply any new accounts with the ready-to-use free certificates. Therefore, the undesigned certificates contained in the certificate database by CMM 342 are similar to the certificates signed by traditional certificate authority 705 in the embodiment of the present invention illustrated in Figure 13 in that they both attach or bind the subject's public key to identity attributes. For example, in the Ramasubramani et al. patent, the CMM 342 assigns the certificates to the particular account by attaching the device ID 316 and other account information.

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/759,443

Filed: January 13, 2001

Docket No.: 10001558-2

Title: PUBLIC KEY VALIDATION SERVICE

The device ID 316 and other account information disclosed in the above passage of the Ramasubramani et al. patent are not equivalent to the public key serial number (PKVN) having a high probability of being different from all previously generated PKVNs as recited in independent claims 1 and 21. Moreover, in amended independent claim 1, the off-line registration authority is configured to generate the first PKVN and amended independent claim 21 includes generating off-line the first PKVN which is not taught by CMM 342 merely receiving the device ID 316 and other account information. As a result, the undesigned issued certificates taught in the Ramasubramani et al. patent which have attached device ID 316 and other account information are in no way equivalent to the unsigned public key validation certificate (unsigned PKVC) issued off-line to a subject that binds the public key of the subject to the first PKVN having a high probability of being different from all other PKVNs generated by the registration authority as included in the limitations of amended independent claims 1 and 21.

Moreover, the Examiner cites the certificate database obtained by CMM 342 in the Ramasubramani et al. patent both for the limitation of the registration authority maintaining a certificate database of unsigned PKVCs in which it stores the first unsigned PKVC and for the table maintained by the credential server that contains entries corresponding to valid unsigned PKVCs stored in a certificate database. The certificate database maintained by CMM 342 in the Ramasubramani et al. patent cannot be both the certificate database of claims 1 and 21 and the table of claims 1 and 21 that contains entries corresponding to valid unsigned PKVCs stored in the certificate database.

In addition, the Examiner asserts that the certificate request (certRequest) signal being sent to the CMM 342 to fetch needed certificates from the certificate database in the Ramasubramani et al. patent teaches the on-line credential server for issuing a disposable public key validation certificate (disposable PKVC) on-line to the subject. As discussed above, however, CMM 342 issues free certificates to minimize the latency of obtaining a certificate with a mobile device and the free certificates which have attached device ID 316 and other account information are in no way equivalent to a disposable public key validation certificate that bind the public key of the subject from the first unsigned PKVC to the first PKVN from the first unsigned PKVC, wherein the PKVN has a high probability of being

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/759,443

Filed: January 13, 2001

Docket No.: 10001558-2

Title: PUBLIC KEY VALIDATION SERVICE

different from all other PKVNs generated by the registration authority as recited in independent claims 1 and 21.

Thus, the Ramasubramani et al. patent does not teach or suggest all of the limitations of independent claims 1 and 21. Furthermore, dependent claims 2-8, 10, 14, and 17-20 further define patentably distinct independent claim 1, and dependent claims 22-28 and 30 further define patentably distinct independent claim 21. Therefore, these dependent claims are also believed to be allowable.

Therefore, applicant respectfully requests that the rejections to claims 1-8, 10, 14, 17-28, and 30 under 35 U.S.C. § 102 based on the Ramasubramani et al. patent be withdrawn and these claims be allowed.

The Examiner rejected claims 37-47 and 49-59 under 35 U.S.C. § 102 (e) as being anticipated by the Perlman et al. U.S. Patent 6,230,266.

The PKI of independent claim 37 includes a first PKVA configured to maintain a record representing the status of validity of the subject's public key. The record has a high probability of being different from all other records of the first PKVA or of any other PKVA. The PKI of independent claim 37 also includes a verifier configured to respond to an authentication of the subject. The authentication includes ascertaining the validity of the subject's public key according to the record of the first PKVA.

The Perlman et al. patent does not teach or suggest all of the above limitations of independent claim 37. The Examiner asserts that passages of the background of the Perlman et al. patent which discuss a traditional certificate authority (CA) teach the limitations of claim 37 of a first PKVA configured to maintain a record representing the status of validity of the subject's public key, and wherein the record has a high probability of being different from all other records of the first PKVA or of any other PKVA. By definition, the PKVA which maintains a record representing the status of the validity of the subject's public key wherein the record has a high probability of being different from all other records of the first PKVA or any other PKVA of claim 37 must be distinct and separate from any certificate authority, such as the certificate authority taught in the Perlman et al. patent or the traditional certificate authorities taught in the present specification, (e.g., certificate authority (CA) 705), which issue certificates that bind the subject's public key to identity attributes of the subject.

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/759,443

Filed: January 13, 2001

Docket No.: 10001558-2

Title: PUBLIC KEY VALIDATION SERVICE

In addition, the PKVA of claim 37 maintains a record representing the status of validity of the subject's public key which is not equivalent to the traditional CA of the Perlman et al. patent generating identity certificates. As stated in the Perlman patent, the CA is used to "know which public key belongs to which principal" (Column 1, lines 65-66) and to verify "the relationship between the public key and the principal to which it belongs" (Column 2, lines 6-7). By contrast, as defined in claim 37, the PKVA maintains a record representing the status of validity of the subject's public key and the authentication by the verifier includes ascertaining the validity of the subject's public key according to the record of the first PKVA, wherein the record has a high probability of being different from all other records of the first PKVA or any other PKVA.

The Examiner also asserts that passages of the background of the Perlman et al. patent discussing an on-line revocation server (OLRS) that maintains a database of certification revocation status information teaches the limitations of claims 37 of a verifier configured to respond to an authentication of the subject, wherein the authentication includes ascertaining the validity of the subject's public key according to the record of the first PKVA. Applicant respectfully notes that the OLRs disclosed in the Perlman et al. patent is similar to the on-line certificate status protocol (OCSP) disclosed in the Background of the Invention section of the Present Application, at page 4, lines 3-12, which operates to permit the verifier of the public key certificate to ask the certificate authority if the certificate is currently valid. The operation of the OLRs disclosed in the Perlman et al. patent and the OCSP disclosed in Present Application which facilitate determining if the certificate is valid are not equivalent to the authentication by the verifier including ascertaining the validity of the subject's public key according to the record of the first PKVA, wherein the record has a high probability of being different from all other records of the first PKVA or any other PKVA as recited in claim 37.

In view of the above, the Perlman et al. patent does not teach or suggest independent claim 37. Furthermore, dependent claims 38-47 and 49-59 further define patentably distinct independent claim 37. Therefore, these dependent claims are also believed to be allowable.

Therefore, applicant respectfully requests that the rejections to claims 37-47 and 49-59 under 35 U.S.C. § 102 (e) based on the Perlman et al. patent be withdrawn and these claims be allowed.

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/759,443

Filed: January 13, 2001

Docket No.: 10001558-2

Title: PUBLIC KEY VALIDATION SERVICE

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected claims 9, 11-13, 16, 29, 31-33, and 36 as being unpatentable over the Ramasubramani et al. patent in view of the Andrews et al. U.S. Patent No. 6,324,645.

In view of the above, the Ramasubramani et al. patent does not teach or suggest all of the limitations of independent claims 1 and 21. Dependent claims 9, 11-13, and 16 further define patentably distinct independent claim 1. Dependent claims 29, 31-33, and 36 further define patentably distinct independent claim 21. Therefore, these dependent claims are also believed to be allowable.

Therefore, applicant respectfully requests that the rejections to claims 9, 11-13, 16, 29, 31-33, and 36 based on the combination of the Ramasubramani et al. patent and the Andrews et al. patent be withdrawn and these claims be allowed.

The Examiner rejected claim 48 under 35 U.S.C. § 103 as being unpatentable over the Perlman et al. patent in view of the Andrews et al. patent.

In view of the above, the Perlman et al. patent does not teach or suggest independent claim 37. Dependent claim 48 further defines patentably distinct independent claim 37. Therefore, dependent claim 48 is also believed to be allowable.

Therefore, applicant respectfully requests that the rejection to claim 48 under 35 U.S.C. § 103 based on the combination of the Perlman et al. patent and the Andrews et al. patent be withdrawn and claim 48 be allowed.

Double Patenting Rejection

The Examiner rejected claims 1-20 under the judicially created Doctrine of Obviousness-Type Double Patenting as being unpatentable over claims 1-22 and 42-47 the Corella U.S. Patent No. 6,763,459

The Examiner rejected claims 21-36 under the judicially created Doctrine of Obviousness-Type Double Patenting as being unpatentable over claims 23-41 and 48-51 the Corella U.S. Patent No. 6,763,459

Applicant has submitted a Terminal Disclaimer with this Response to overcome the above double-patenting rejections. Therefore, Applicant respectfully requests that the above

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/759,443

Filed: January 13, 2001

Docket No.: 10001558-2

Title: PUBLIC KEY VALIDATION SERVICE

double-patenting rejections to claims 1-20 and 21-36 based on the Corella patent be removed and that these claims be allowed.

CONCLUSION

In view of the above, Applicant respectfully submits that pending claims 1-14, 16-34, and 36-59 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-14, 16-34, and 36-59 is respectfully requested.

No fees are required under 37 C.F.R. 1.16(b)(c). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 08-2025.

The Examiner is invited to contact the Applicant's representative at the below-listed telephone numbers to facilitate prosecution of this application.

Amendment and Response

Applicant: Francisco Corella

Serial No.: 09/759,443

Filed: January 13, 2001

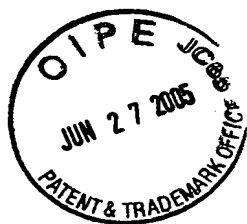
Docket No.: 10001558-2

Title: PUBLIC KEY VALIDATION SERVICE

Any inquiry regarding this Amendment and Response should be directed to either Patrick G. Billig at Telephone No. (612) 573-2003, Facsimile No. (612) 573-2005 or William J. Streeter, Esq. at Telephone No. (970) 898-7247, Facsimile No. (970) 898-3886.

In addition, all correspondence should continue to be directed to the following address:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400



Respectfully submitted,

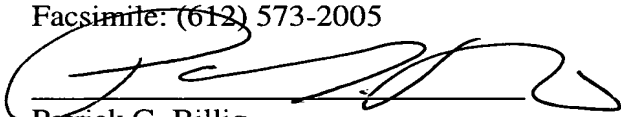
Francisco Corella

By his attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2003
Facsimile: (612) 573-2005

Date: 6-24-05

PGB:cmj


Patrick G. Billig
Reg. No. 38,080

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this paper or papers, as described herein, are being deposited in the United States Postal Service, as first class mail, in an envelope address to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 24 day of June, 2005.

By 

Name: Patrick G. Billig